DVB TECHNICAL MODULE SUB-GROUP ON COPY PROTECTION TECHNOLOGIES

CALL FOR PROPOSALS FOR CONTENT PROTECTION & COPY MANAGEMENT TECHNOLOGIES

Introduction

The DVB Commercial Module has issued commercial requirements for a new DVB Content Protection and Copy Management (DVB CPCM) system to provide a common framework for the protection and management of content beyond the traditional boundary points of DVB compliant CA systems. The new scope particularly encompasses the In Home Digital Networks and Personal Video Recorder technologies where content is moved and recorded on devices that have heretofore not been a focus of the DVB Project.

The DVB TM ad-hoc group on Copy Protection Technologies is issuing this Call for Proposals to elicit technology proposals to meet the commercial requirements generated by the DVB Commercial Module. The documents issued by the DVB CM outlining these requirements are attached to this document as annexes.

CALL FOR PROPOSALS FOR CONTENT PROTECTION & COPY MANAGEMENT TECHNOLOGIES

1 Background information

DVB (Digital Video Broadcasting) is a consortium of around 300 companies in the fields of Broadcasting, Manufacturing, Network Operation and Regulatory matters that have come together to establish common international standards for the move from analogue to digital broadcasting. This common market-led initiative has resulted in DVB becoming a prominent and leading international standard and the sole choice for technologies that enable an efficient, cost effective, easy/rapid transition, higher quality and interoperable digital broadcasting.

The DVB Project Office and its 3.5 staff are based in Geneva, Switzerland. It is the nucleus of the Administration and Marketing Communications of the Consortium. See also http://www.dvb.org

1.1 DVB CPCM Activity

The DVB Commercial Module has issued commercial requirements for a new DVB Content Protection and Copy Management (DVB CPCM) system to provide a common framework for the protection and management of content beyond the traditional boundary points of DVB compliant CA systems. The new scope particularly encompasses the In Home Digital Networks and Personal Video Recorder (PVR) technologies where content is moved and recorded on devices that have heretofore not been a focus of the DVB Project.

The DVB Technical Module sub-group on Copy Protection Technologies is issuing this Call for Proposals to elicit technology proposals to meet the commercial requirements generated by the DVB Commercial Module. The documents issued by the DVB CM outlining these requirements are attached to this document as annexes.

1.2 How DVB standards are developed

For each specification, a set of User Requirements is compiled by the Commercial Module. These are used as constraints on the specification. User requirements outline market parameters for a DVB system (functionality, extensibility, etc.).

The Technical Module then develops the specification, following these user requirements. The approval process within DVB requires that the Commercial Module supports the specification before it is finally approved by the Steering Board.

The work within the DVB groups is open to all DVB members. In the technical groups, most work aims at achieving consensus between all participants.

Following approval by the Steering Board, DVB specifications are offered for standardisation to the relevant international standards body (ETSI or CENELEC), through the EBU/ETSI/CENELEC JTC (Joint Technical Committee), the ITU-R, and ITU-T.

1.3 DVB principles of standardisation

The standardisation efforts within the DVB project are characterised by the following principles:

- Openness

  DVB systems are developed through consensus in the working groups of the Technical Module. Members of the groups are drawn from the general assembly of the project. Once standards have been published, through ETSI (http://www.etsi.org), they are available at a nominal cost for anyone. Open standards allow manufacturers and broadcasters to implement innovative and value added services. The DVB technology is made available world-wide irrespective of the location of its development.

- Interoperability

  Because the DVB standards are open, all the manufacturers making compliant systems are able to guarantee that their DVB equipment will work with other manufacturers' DVB equipment, enhancing the value of the CE devices to the consumer. In addition, because the standards are designed with a maximum amount of commonality, and are based on the common MPEG-2 coding system, they may be effortlessly carried from one medium to another, which is frequently needed in today's complex signal distribution environment. DVB signals move easily and inexpensively from satellite to cable, from cable to terrestrial and between consumer devices.

- Flexibility

  Owing to the use of MPEG-2 packets as "data containers", and the critical DVB Service Information surrounding and identifying these packets, DVB can deliver to the home almost anything that can be digitised, whether this is High Definition TV, multiple channel Standard definition TV (PAL, NTSC or SECAM) or even exciting new broadband multimedia data and interactive services provided by the DVB Multimedia Home Platform.

- Market-led initiative

  In contrast to earlier initiatives in Europe and the United States, the DVB Project works to strict commercial requirements established by organisations who work every day to meet its needs. It is not a regulator- or government-driven (top-down) initiative. Working to tight timescales and strict market requirements means achieving a considerable economy of scale, which ensures that, in the transformation of the industry to digital, broadcasters, manufacturers and, finally, the viewing public will benefit.

1.4 DVB work in Content Protection and Copy Management

The DVB has developed specifications in the area of Conditional Access, which have found a broad usage globally (see: http://www.dvb.org/standards/index.html). The emerging Digital Video Recorder technology and the continuing digital convergence has triggered new DVB work in the area of Content Protection and Copy Management technologies. The first step in the DVB process is to produce a Commercial Requirements document. This work has been conducted in the DVB Copy Protection (DVB-CP) group set up by the Commercial Module. The result of this work is the DVB-CP Summary of Requirements - (see Annex 1) and the DVB-CP Table of Abbreviations (Annex 2), which summarise the specific commercial requirements of the DVB Content Protection and Copy Management (DVB CPCM) system.

The DVB Technical Module (DVB TM) has the responsibility to develop technical specifications that meet the Commercial Requirements. It has established a sub-group, the DVB Copy Protection Technologies (DVB CPT) group, to do the specification drafting work. The DVB CPT reports regularly to the TM.

The DVB CPT has started its work by drafting this Call for Proposals. The proposals will form the starting point for the DVB CPT specifications that should meet the DVB CPCM commercial requirements.

2 Abbreviations and Glossary

This document employs the abbreviations and glossary that form part of the commercial requirements documents of the DVB Commercial Module's Copy Protection sub-group. These documents form an annex of this document.

In addition, some other terms have been used and these are defined below:

2.1 Abbreviations

API	Application Programming Interface
CAS	Conditional Access System
DRM	Digital Rights Management
RG	Residential Gateway

2.2 Glossary

Application Programming Interface:	the software interface exposed by the DVB CPCM system to any proprietary plug-ins.
Residential Gateway:	a device that bridges the external, access network and a home network

3 Architecture for communication and use of DVB CPCM Usage States

Figure 1 below shows a basic consumer domain architecture and how it might connect to the outside world for content distribution and consumption. The diagram is only a single example – we recognise that many different permutations are possible and likely.

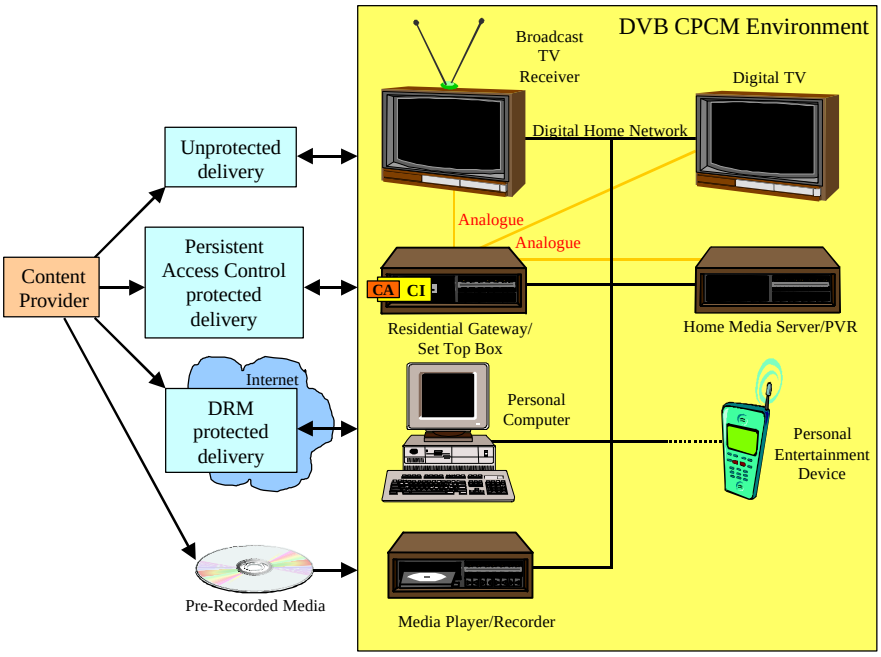

Figure 1 - Consumer domain architecture

In Figure 1, the following clarifications are made, based on the DVB-CP Summary of Requirements:

1. The content is delivered from Content Providers through Service Providers to the Consumer using a variety of delivery means, including unprotected, protected (such as Conditional Access System (CAS) and/or Digital Rights Management (DRM)) and pre-recorded media.
2. Where content enters the DVB CPCM environment, it may move from a traditional protection mechanism such as through a Residential Gateway (RG) or Set Top Box (STB) border device using the DVB Conditional Access (CA) system (and possibly across the DVB Common Interface (CI)) into the DVB CPCM environment. . It should be recognised that control of content protected by a CAS may or may not be handed off to the Baseline DVB CPCM system. It is also possible that the content enters through an unprotected environment (e.g. over a free-to-air public broadcast) before entering the DVB CPCM environment. Regardless of how the content enters the consumer's Authorised Domain, the DVB CPCM system shall provide end-to-end protection of the content and its related Usage States through the point of consumption by the end user
3. The Baseline DVB CPCM system shall provide support for the four copy control usage states of Copy Control Not Asserted, Copy Once, Copy No More, and Copy Never. In addition, the Baseline DVB CPCM system must also provide a means of indicating whether content may be Moved for Consumption outside the consumer's Authorised Domain and the necessary protection mechanism for supporting this function. The Authorised Domain may also include devices not physically attached to the Digital Home Network (e.g. portable entertainment device or remotely connected device).
4. Due to the existence of, and the need to support, legacy analogue devices, the DVB CPCM system must provide protection of content, to the extent possible, flowing across both analogue and digital interfaces between devices within the consumer's Authorised Domain. The DVB CPCM system

specification must describe a mechanism by which the defined DVB CPCM Usage State information can be mapped for carriage on the analogue signal and can trigger “market accepted” analogue protection systems.

5. Persistent Content Protection implies that the protection is maintained over time until such time as deemed appropriate by the provider of such protected content (e.g., the Pay TV Broadcaster using a proprietary CA system), whence the protection may be relinquished to others. The persistent content protection given by the Conditional Access system generally provides both access control to, and copy control for, the content. When its content business/consumption model specifies, the CA system may pass access control and copy control responsibility to the DVB CPCM system. This enables the CA provider to offer rental paradigms for content it protects and which may exist on horizontal storage devices. Note that DRM naturally implies the persistence of protection by its very nature.
6. The DVB CPCM system will define and support a standardised digital interface at a logical level, establishing mutual trust between devices that allows protected content, Usage State information, and the control of content usage to be securely exchanged between two or more DVB CPCM compliant devices.

4 Envisaged scenarios for DVB CPCM applications

4.1 Delivery of unprotected and unmarked content into the home

Where content is not protected or marked in any way in terms of intended usage restrictions as it enters the home, the DVB-CP Summary of Requirements document (Annex 1) requires the association of some default Usage States with such content. In particular, the content is assumed to be marked i) “Copy Control Not Asserted” and ii) “Movement for Consumption Outside the Authorised Domain Allowed”. In this case, no technological restrictions are placed on the duplication of the content. This does not mean that copyright ownership is transferred in any way or that rights under copyright are waived.

4.2 Delivery of unprotected but marked content into the home

Content may also enter the home unprotected, but marked in a way such that Usage States are associated with it. This may be facilitated through the use of associated and/or embedded data that carries Usage State information. In this case, the DVB CPCM system should continue to associate these DVB CPCM defined Usage States with the content and honour them.

4.3 Delivery of protected content into the home

In the case when content is protected by some scheme and this content arrives at the home, it may be delivered into the DVB CPCM environment via some border device that straddles both protection systems. This device is responsible for mapping the equivalent to usage states of the external system into the Usage States of the DVB CPCM system. Examples of this include broadcast content protected and managed by a proprietary Conditional Access System (CAS) and passed to the DVB CPCM environment (and possibly across the DVB Common Interface (DVB CI)), pre-recorded media containing protected content, , Internet-delivered content managed and protected with a Digital Rights Management (DRM) system, etc. The DVB CPCM system API should facilitate the interoperation with a wide variety of trusted non-DVB CPCM systems.

4.4 Extension of the Authorised Domain to remote devices

We also envisage a scenario where authorised users are located outside of their home (i.e. office, holiday home, etc.). In the case where the user has a DVB CPCM compliant device at this remote location, it shall be possible to extend the Authorised Domain securely to this device.

4.5 More extensive CPCM systems

We acknowledge that the DVB CPCM environment may extend back up the supply chain, right as far as the Content Provider. This does not change the protection and mapping function of the border device that provides the DVB CPCM wrapper to protect content. It is merely likely to be a device that offers a different suite of functions than, say, a Set Top Box.

4.6 Multiple non-DVB CPCM protection systems

The following diagram provides a reference model for the DVB CPCM system:

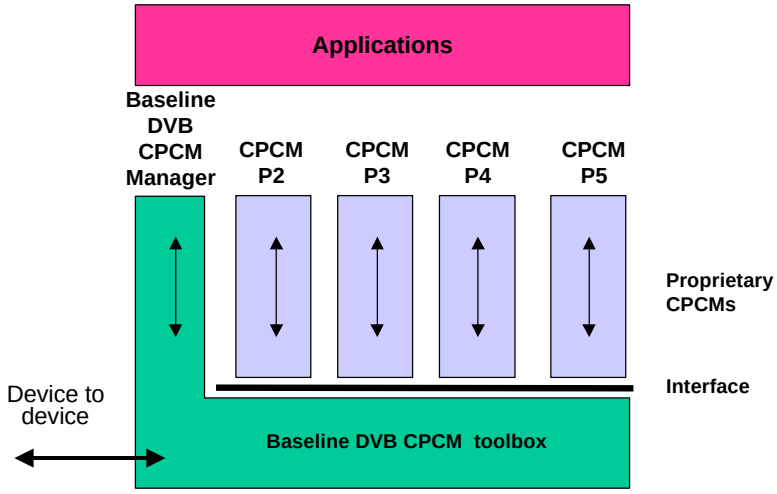

Figure 2 - DVB CPCM Functional Model

It comprises a DVB CPCM framework of tools which are used by the Baseline DVB CPCM system and can also be called on by a plurality of proprietary CPCM plug-ins ("Proprietary CPCMs"). The Proprietary CPCMs connect via a standardised interface to the Baseline DVB CPCM tools.

It is envisaged that the DVB CPCM tools and Baseline DVB CPCM Manager will be resident in every DVB CPCM compliant device to which the DVB CPCM system is to be applied. The Proprietary CPCMs will comprise either downloadable, tamper resistant software delivered via a secure channel or be robustly implemented in hardware.

It is thus expected that DVB CPCM system will support the following functions:

- A tool to securely transfer content from one Baseline DVB CPCM compliant device to another.
- A tool to securely deliver Usage States and control data from one Baseline DVB CPCM compliant device to another.
- A mechanism to allow two Baseline DVB CPCM compliant devices to establish mutual trust.
- A standardised logical interface linking Baseline DVB CPCM compliant devices to support the above.
- An API that allows applications to interact with the Baseline DVB CPCM system.
- The ability of the Proprietary CPCMs to hand over or retain control of content delivered through the DVB CPCM system.

This is not necessarily an exhaustive list of the functionality encompassed by the elements of the functional model.

4.7 Extending the capabilities of the Baseline DVB CPCM systems

Proprietary Content Protection and Copy Management systems are likely to exceed the capabilities of the Baseline DVB CPCM system in terms of range of usage states and business models supported. There are at least two scenarios that come to mind for extending the capabilities of the Baseline DVB CPCM system:

4.7.1 Adding functionality to the Baseline DVB CPCM system

The Baseline DVB CPCM system needs to be extensible so that functionality of the DVB CPCM system itself can be enriched to accommodate more business models in the future. The inherent difficulty we see with this is that such extensions would ideally be made common in format wherever they are introduced into the Baseline DVB CPCM system, but this may require a central authority to administer. It would be preferable to avoid the need for such an entity.

4.7.2 Transactional APIs

Another possibility is for the Baseline DVB CPCM system to revert copy control decisions beyond its understanding to an external, proprietary Content Protection and Copy Management system. This calls for a bi-directional API with transaction support and some means of indicating that the Baseline DVB CPCM system should use this authority outside.

At the same time, there needs to be a means of informing the consumer of the actual usage situation for any piece of content that falls into this category. The external, proprietary DVB CPCM system will pass information through the DVB CPCM environment so that the consumer can be presented with the proper usage requirements for some content.

5 Binding Usage State with content

Usage States for a piece of content are tightly bound to that content. This binding may be logical such that it is clear what Usage States pertain to which piece of content even though they may not be co-located. Alternatively, it may be a requirement that they be physically bound and hence co-located. It is likely that a hybrid of these two arrangements will prevail.

5.1 Physical binding of Usage States to content

In the case where content is always physically bound to the Usage States, there needs to be a mechanism for securely attaching and transporting the Usage States with the content and securely determining the suitability and identity of the recipient for being entrusted with the content and enforcement of the Usage States. It is likely that some devices will not offer as rich a set of Usage States as others and such mismatches should be dealt with gracefully. Proposals are sought on managing this relationship.

5.2 Logical binding of Usage States to content

For content that is only logically bound to the Usage States, it is probable that a secure, central repository of Usage States and the interpretation of these will exist in the DVB CPCM system. Mechanisms may exist to support querying these repositories for permission to perform actions on the content in accordance with the Usage States. The process of reliably and securely issuing a query and handing back a response needs to be addressed.

6 Issues to be Addressed by Proposals

This section contains descriptions of issues that the DVB CPT considers to be important for proposals in addition to the Commercial Requirements. Proposals are encouraged to address these issues as far as they apply to the proposal. Specific paragraphs are reserved for the discussion of these issues in the Format of the Proposal described in section 8.

It is noted here that the requirements in this document may be conflicting, nonetheless proposals should seek to fulfil any requirement as far as feasible.

6.1 Backward compatibility

As expressed in DVB Commercial Requirements, compatibility with legacy DVB products, which represent the installed base of consumer equipment, is essential in order to not slow down the PVR emerging market and, to not jeopardise the credibility of DVB standards. This means that, for broadcast services at least, the DVB CPCM system shall allow backward compatible implementation. When required by the network operator, the modified signal, including controls for DVB CPCM mechanism in CE devices, shall be correctly decoded and displayed by the currently deployed STB base without a significant increase of necessary data rate (for example DVB Simulcrypt is possible, replicating the content stream in different formats is excluded).

6.2 Differentiating factors

In areas where proposals use common or widely used techniques (e.g. encryption, key exchange) proponents should describe the specific strength or advantage of the chosen technology for the purpose of the DVB CPCM system.

6.3 Scalability, Upgradability, and Renewability

Proposals may specify extension mechanisms to offer different levels of protection. The extensions may provide scalability, upgradability and/or renewability. In order to achieve world-wide applicability, it should be noted that certain levels of protection might not be legally acceptable in some regions. Such extension mechanisms may also provide for the longevity of the DVB CPCM system, as a higher level of protection may have to be introduced over the lifetime of the technology, taking into account a lifetime of 10 years for consumer products. All proposals should address the mechanism for renewability in the case of a successful attack at both the device level and system wide.

6.4 Management of Secrets

Where proposals specify the use of unique secrets for devices, software components or content objects, it must be stated, how the infrastructure for managing and maintaining such secrets could be established.

6.5 Complexity, Performance, Level of Protection and Maintenance

Proponents should give measures for the complexity and performance of an implementation for specified technology as far as it can be defined/evaluated/measured. Possible measures could be gate count for silicon implementations or runtime benchmarks for software implementations.

Proposals should describe how the specified solution can maintain security and consistency of protection in the heterogeneous environment established by an open market.

Proposals should provide some analysis of security of the proposed technology and susceptibility to attack.

It is well understood that the implementation costs of such a system are sensitive issues for the CE manufacturer, technology provider, content distributor and content provider and should not be prohibitive to its widespread adoption. Complexity of implementation and technologies must therefore be chosen with care.

6.6 Tamper Evidence of Content or Usage States

In order to establish consistent protection even in partially compromised environments it is desirable to include technologies that provide tamper evidence on content and/or meta-data.

Where such tampering is reliably detected, the default state of “Copy Never” should be asserted. The likelihood of false (positive and negative) detection as an important performance criterion should be given.

6.7 Maturity and Completeness of proposed Technologies

It is encouraged that proposals use existing and proven technologies. It is desirable to make reference to existing standards/specifications/technologies as far as possible.

Proponents are not required to address the complete DVB CPCM system, i.e. proposals that conform to subsets of the CP requirements will be considered as potential components to the DVB CPCM specification.

7 Procedure for submissions and evaluation

7.1 The process followed by the DVB CPT

The process that the DVB CPT has decided to follow is to issue a Call for Proposals for Content Protection and Copy Management technologies. The Call is open for responses to DVB Members, as well as to non-members. If such non-members have relevant technologies they can issue a response. In some cases such a response will be informative, but it may also be a proposal for some technology. In the latter case, the proposer needs to join DVB to advance the use of the proposed solution into a DVB specification. The DVB CPT would like to receive two types of submissions:

7.1.1 Information Papers

This document also serves as a Call for Information, as it encourages organisations to inform the DVB CPT group about relevant activities in the world. This is useful, as DVB has always taken notice of other standardisation activities and of market forces. In the area of Content Protection and Copy Management technology, many non-broadcast technologies may be relevant. As this is outside the direct view of most DVB members, contributions informing the DVB CPT of relevant activities in related areas are particularly welcome.

7.1.2 Technical Papers

Some organisations may have a well-defined idea about the technological elements that are needed to meet the Commercial Requirements. Contributions that outline such a Baseline DVB CPCM System and also extensions to the Baseline DVB CPCM system are invited and such inputs may serve as the basis for a DVB CPT specification.

7.2 Reporting of results

The responses to the CfP will be discussed at a two-day meeting of the DVB CPT group according to the timeline in section 7.3. A representative of each submission is invited to present the proposal at this meeting. After the presentations the DVB CPT will start its drafting work.

7.3 Timeline

21 September 2001	Contributors are requested to communicate their intention to submit a proposal to the DVB CPT by 12h00 Central European Time on this date. Proposers will receive a submission number and be allocated a timeslot to present their proposal at the November DVB CPT meeting. Presentations of papers without notification might be shorter.
19 October 2001	Deadline for Submissions (by 12h00 Central European Time on this date).
13-15 November 2001	Proposers Presentation to the DVB CPT meeting in Geneva, Switzerland.

7.4 General terms and conditions

The DVB CPT will not consider submissions that contain detail that is Company Proprietary or Confidential. Those submitting information acknowledge that any and all information contained in their submission will *not* be treated as confidential and should not be marked as such.

Acceptance of submissions does not imply that the information will be included in any DVB specification.

7.5 Liaison with other DVB bodies

The DVB is a complex organisation. In some cases it is conceivable that some parts of the DVB CPT specification actually can benefit from the expertise of other expert groups within the DVB project. This liaison is handled by the DVB Technical Module.

7.6 Submission Details

The responses (both the intention to submit and the actual submission) to this Call should be by email before the appropriate deadlines to both the chairperson of the DVB CPT (wmooij@irdetoaccess.com) and to the DVB project office (melamed@dvb.org). Documents should be attached in one of the following formats: MS-Word, HTML or PDF. The DVB reserves the right not to accept requests received after the deadlines for either requests to respond or document sumissions.

7.7 Requests for clarification of this Call for Proposals

All questions relating to the meaning or intention of text contained in this CfP should be addressed to Guy Hirson (mailto://guy.hirson@ntl.com). All responses will also be copied to the DVB CPT reflector for further review by the sub-group.

8 Format of the proposal

In order to speed up the evaluation of the submitted papers, proposers are requested to use the format described below.

8.1 Table of Contents

Contact details

IPR statement

Executive summary

Description of the architecture

Functional areas addressed

etc...

8.2 Contact details for proposer

Individual contact name

Organisation

Telephone

Fax

Email

Postal address

8.3 Executive summary of the proposal

A brief description of the proposal, in non-technical terms, should be provided. This should be less than 500 words.

8.4 Description of the architecture of the proposal

The complete system that falls within the scope of the DVB CPCM is very complex and can be made of several distinct parts. Proposals for partial solutions will be considered. A description should be given that identifies which parts of the overall DVB CPCM infrastructure are addressed.

8.5 Functional areas addressed

The functions required of the DVB CPCM can be grouped into several different functional categories. If relevant to your proposal, descriptions of functional categories in your proposal can be included. Typical examples are:

Verification of recipient

Confirmation of the identity of the recipient

Matching the rights of the recipient with the requirements of the content

Determination of the security capability of the recipient

Verification of source

Confirmation of the identity of the content source

Prevention of rogue feeds of content

Protect against malicious attempts to alter content already received

8.6 Protection mechanism for content

Proposed algorithms and functions

How are usage states/rules supported?

What levels of security does your proposal support?

Does your proposal provide end-to-end protection of the content?

How robust is the protection mechanism to adversarial and inadversarial attack

How does the mechanism recover from bit and burst errors

Does your proposal rely on any interfaces (for example IEEE 1394, HiperLAN, SMPTE 259M) or any modifications to such interfaces, (for example the use of previously undefined data fields)

Does your proposal rely on transport requirements such as a return channel?

Does your proposal include the use of a return channel if it is available?

Does your proposal support both content entering through protected as well as unprotected means?

8.7 DVB CPCM API

How does you DVB CPCM API support multiple CA systems?

How does you DVB CPCM API support multiple proprietary DVB CPCM plug-ins?

How does it identify the need to hand control to a specific Proprietary CPCM?

8.8 Underlying security infrastructure

Typical examples: key exchange, Secure Authenticated Channels

Does your proposal have transport requirements including a return channel?

Does it have APIs and plug-in support?

How is the interface between different CPCM and CA systems managed?

8.9 Implementation requirements

How much RAM, ROM, and processing power does your proposal require?

Please specify any special requirements your proposal makes on hardware (e.g. secure silicon).

If relevant, how long does your proposal take to operate (for example, amount of time required to establish a secure channel)?

What is the estimated cost of the hardware and/or software footprint?

If relevant, what additional data transport capacity does your proposal require?

What is the maintenance complexity for your proposal?

8.10 Usability

What human intervention or interaction does your proposal require (for example, insertion of smart card, entry of passwords, credit card details)?

8.11 Renewability, revocation and resistance to obsolescence

The way in which the DVB CPCM system can be upgraded or renewed should be described.

A description of foreseeable circumvention devices and defences against them should be given. This should include the type and complexity of devices that could be used to circumvent the system.

The process of revoking hacked or cloned devices for specific services must be described.

A discussion on scalability and robustness of security should be provided.

8.12 Suitability for import or export

It is known that certain cryptographic techniques have restrictions on import and export in certain countries. Any relevance of these restrictions to your proposal should be stated.

8.13 Current state of development

Please state in what form your proposal is currently available, for example, as an algorithm description, software modules, real-time demonstrator, or off-the-shelf commercial products.

8.14 IPR statement

Proposals shall be accompanied by a statement that any intellectual property rights will adhere to the DVB IPR policy as formulated in the relevant sections in the DVB Memorandum of Understanding.

8.15 Conformance statement

An annotated copy of the summary table of requirements indicating which requirements your proposal meets should accompany your proposal.

8.16 Other information in support of your proposal

Please use this section to describe any special features of your proposal not covered by the above sections.

Annex 1 DVB-CP Summary of Requirements (DVB-CM283)

No.	AREA	REQUIREMENT
1	Environment	The DVB CPCM system shall be capable of providing end-to-end protection for content in all processes from the point of initial distribution to the end user through to the point of consumption by the end user.
2	Environment	The termination point of the DVB CPCM system shall be the point of viewing/listening by the end user unless the display can output the Content in digital form.
3	Environment	The DVB CPCM system shall be applicable to the widest possible range of equipment (and not just restricted to DVB-specified systems or sub-systems).
4	Environment	The DVB CPCM system shall be independent of the delivery mechanisms (i.e. transport media/protocols): e.g. the system should be applicable to content received via the cable, terrestrial and satellite systems, the Internet or pre-recorded media.
5	Environment	The DVB CPCM system shall interact with other CPCM systems in a manner such that the rights delivered with the content are preserved.
6	Environment	The DVB CPCM system shall function with or without a CA system whose function is to deliver protected content to the consumer.
7	Environment	The DVB CPCM system shall not rely on the availability of a live return data-channel to the content/service provider but may rely upon it if a service provider chooses to operate their domain in this way.
8	Functionality	The DVB CPCM system shall be capable of protecting all DVB stream-types, including subtitling, teletext, object and data carousels, and private data. The priority is to protect the primary picture and sound of television services.
9	Framework	The specified DVB-CPCM-Baseline-System shall be able to provide content providers with the necessary protection for their content.
10	Framework	The authorised Copying, Moving and Consumption (“Authorised Usage”) of content protected by the baseline DVB-CPCM system shall be described by Usage State Information which shall be tightly bound to the content.
11	Framework	The DVB CPCM system shall include a generic framework which supports a plurality of proprietary CPCM plug-ins which can be used by any device conforming with the DVB CPCM specification.
12	Framework	There shall be a DVB-specified interface between the CPCM generic system and the proprietary plug-ins.

13	Functionality	The baseline DVB CPCM system shall support the following Usage States as defined in the Glossary: Copy Control Not Asserted Copy Once Copy No More Copy Never A secure mechanism shall be provided whereby an authorised and authenticated agent may change, subsequent to delivery, the Usage State associated with an item of content from any Usage State to any other Usage State unless the content is marked “Change of Usage State is not permitted”. The baseline DVB CPCM system shall also support a means of indicating whether protected content may be Moved for Consumption outside the Authorised Domain. Rights owners may use a “Usage State Extension” to specify additional rules for the Authorised Usage of the Content. The content of such Usage State Extensions may be proprietary (i.e. not specified by the DVB) and shall be capable of being decoded only by the appropriate proprietary plug-in connected to the DVB baseline CPCM via the DVB standardised interface. Devices which do not have the appropriate plug-in fitted shall interpret Content with any such Usage State Extensions as “Copy Never” and shall respond accordingly. N.B. Proprietary plug-ins shall not require capabilities or resources in the baseline DVB-CPCM system beyond those needed to implement the baseline DVB-CPCM system.
14	Framework	It shall be possible for a device to pass control of: (a) content; and (b) CPCM to another qualifying CPCM device provided that the same has an appropriate interface with the DVB CPCM system.
15	Framework	The DVB CPCM system shall not allow one proprietary CPCM plug-in to circumvent or modify another one.
16	Framework	The baseline DVB CPCM system shall not be subverted by proprietary CPCM systems.
17	Framework/ Security	Access to the DVB CPCM by plug-ins shall be subject to authentication of each plug-in.
18	Framework	The requirements that a downloadable proprietary CPCM plug-in has of the target device (e.g. memory-space) must be specified.
19	Framework	The DVB CPCM system shall support the definition and use of "domains" and the application of Usage States associated with each item of content to control movement and copying within and across domain boundaries. A mechanism is required for securely defining and implementing “Authorised Domains”.
20	Framework	DVB CPCM compliant devices, including those which do not use on-line authentication, shall be capable of being denied specific content in accordance with a revocation list.
21	Functionality	The DVB CPCM system shall enforce limitations of use and copying of the content in accordance with the Usage States Information conveyed with the content.
22	Functionality	The DVB CPCM system shall provide a means whereby the rights-protection state and associated usage rules of each item of content can be signalled to each viewer clearly and unambiguously both before and after recording.

23	Functionality	The DVB-CPCM system shall allow recording of transmissions or downloads of “Copy Once” content. When a Copy is made of this content, original download will either be deleted or made inaccessible and the Copy of the Content will be re-marked “Copy No More” such that the copy is protected in a manner to prevent further copying. N.B. For the avoidance of any doubt, the requirement to modify the Usage State “Copy Once” to “Copy No More” applies only to devices which are capable of creating Copies and not to devices which can only playback and/or display the Content.
24	Functionality	The DVB CPCM system shall allow "Copy No More" content to be Moved from one storage device to another (but not Copied) (e.g. Moving a piece of music from a hard disc store to a portable memory module for on-the-move listening) provided that such a device is in the same Authorised Domain.
25	Functionality	The DVB CPCM system shall not debar the presentation of information to the end user about the extent of copying and serial copying that is allowed for each programme or content object making up such a programme
26	Functionality	The DVB CPCM system must provide protection of content (such that, to the extent possible, only the use authorised by the Usage States Information is permitted) flowing across/between both analogue and digital interfaces/interconnections/devices within the Authorised Domain.
27	Functionality	The DVB CPCM system shall support all known forms of scheduling and payment systems including VoD and be flexible enough to allow new business models to be developed.
28	Functionality	The functionality of the DVB CPCM system shall be scalable to reflect the capabilities of the connected devices e.g. devices without persistent storage capability shall have simpler CPCM functionality
29	Functionality	The renewable security elements of the DVB-CPCM system shall all be capable of being renewed at an economic cost throughout the lifetime of the relevant CE equipment
30	Functionality	Usage rules for proprietary plug-in modules to the DVB-CPCM systems may be conveyed by downloadable data/applications. The DVB-CPCM system shall support the conveyance of private/proprietary data to proprietary plug-in modules.
31	Functionality	The DVB-CPCM system shall allow the user to Move content that they have an entitlement to view/store from one storage medium to another for the purpose of replacing or upgrading equipment.
32	Functionality	Any watermarks embedded in the content will be passed through the end-to-end DVB system in the same manner as content. No special consideration will be given to the handling or processing of embedded watermarks by the DVB-CPCM (except for any watermarking defined as a component of the DVB-CPCM system by CPT). It will be the responsibility of the non-DVB-CPCM watermark technology provider/user to ensure that their watermarks are robust enough to pass through the DVB-CPCM system.
33	Performance Measures	The DVB CPCM system shall not introduce any perceptible degradation of content quality as perceived by the majority of end users; (Requirement to be quantified by DVB-CPT Technical Group).
34	Performance Measures	The DVB CPCM system shall not introduce unacceptable delays in delivery of content as perceived by the majority of end users nor any impairment to the synchronisation of picture, sound and data services. (Requirement to be quantified by DVB-CPT Technical Group).
35	Robustness	The transmission of the DVB CPCM Usage States Information must be as robust as that of the content which it protects.

36	Robustness	The transmission of the Usage States Information must survive transcoding of the transport streams to a lower bit-rate and other normal digital distribution processes.
37	Security	The DVB-CPCM system should be designed such that the requirement for making devices tamper-proof and tamper-evident is minimised and localised to those elements (e.g. secure chips) which hold cryptographic secrets and not extended to requiring physical security of the whole device. It is, nevertheless, acknowledged that in implementing the DVB-CPCM system making devices tamper-proof and tamper-evident would be an important contribution towards security.
38	Security	Management of cryptographic secrets (if any) in the DVB CPCM system shall not require that a single overall centralized licensing authority is established and used.
39	Security	Management of cryptographic secrets (if any) in the overall DVB CPCM system may require the use of device revocation in instances of cloned, stolen or lost device keys but such device revocation shall be in respect of a particular service or group of services and shall not inhibit the operation of the device entirely.
40	Security	If content is does not include recognisable DVB-CPCM information the appropriate Usage Rule shall be deemed to be “Copy Control not Asserted”.
41	Security	If the DVB-CPCM information associated with an item of content is found to be corrupted or unintelligible due to errors (but still recognisable as DVB-CPCM information) the appropriate Usage Rule shall be deemed to be “Copy Never.”
42	Compatibility	The DVB-CPCM shall be backwards compatible with legacy devices to the extent possible without compromising functionality or security or adding significant to the cost.
43	Inter-Device Interfaces	The DVB-CPCM specification must define a standardised external digital interface between DVB-CPCM compliant devices such that: (a) protected content; (b) Usage States Information; and (c) control of content usage can be securely exchanged between two or more DVB-CPCM devices. A means must be provided to establish trust prior to secure exchanges between CPCM compliant devices. [1]
45	Levels and Profiles of the DVB-CPCM baseline system	The DVB-CPCM baseline system shall initially comprise a single profile and level. However, to the extent possible without adding significantly to cost and/or delay in implementation, consideration should be given to facilitating the future provision of additional levels and profiles to the DVB-CPCM system in a way which is backwards compatible with the original single profile and level.

[1] MPA proposes to add [not agreed]: “This Inter-Device interface shall be mandatory on all DVB-CPCM compliant devices: DVB-CPCM devices which do not have this type of interface may have limited access to high value content.”

Annex 2, DVB-CP Table of Abbreviations and Glossary (DVB-CM282)

1 Table of Abbreviations

	Abbreviation	Term
1.	AC	Access Control
2.	CA	Conditional Access
3.	CE	Consumer Electronics
4.	CPCM	Content Protection and Copy Management
5.	DES	Data Encryption Standard
6.	DSA	Digital Signature Algorithm
7.	DTV	Digital TeleVision set
8.	DVB	Digital Video Broadcasting
9.	ECM	Entitlement Control Message
10.	EMM	Entitlement Management Message
11.	EPG	Electronic Program Guide
12.	HSM	Host Security Module
13.	IPR	Intellectual Property Rights
14.	IDTV	Integrated Digital Television
15.	MHP	Multimedia Home Platform
16.	SAC	Secure Authenticated Channels
17.	STB	Set-Top Box

2 Glossary

1.	Term	Meaning
2.	Access Control	The process of ensuring that content is accessed only by those entities authorised to do so, and only in a manner for which they have been authorised.
3.	Acquisition	Retrieval of content for local storage and/or usage.
4.	Adversarial Attack (Active)	An attack by an entity on a system, the purpose of the attack being to steal information, to inject false information into the system, or to corrupt information already present in the system. See also Inadversarial Attack.
5.	Archive	A Move of the original for the purposes of preservation of the content. The copy protection status shall not be altered by the Archiving

6.	Asymmetric Encryption	Type of encryption in which encryption keys are different from decryption keys, and one key is computationally difficult to determine from the other.
7.	Audit Trail	A process that provides a date and time stamped record of the usage of a system. Itrecords what a device was used for, allowing a security manager to monitor the actions of every user, and can help in establishing an alleged fraud or security violation. N.B. some users and equipment may not be accessible for audit
8.	Authentication (Message)	Message authentication: provides assurance about the identity of the sender (timeliness guarantee).
9.	Authentication (Entity)	Entity authentication: provides assurance about the identity of the sender and his active participation (timeliness guarantee).
10.	Authorised Domain	The devices, networks and interfaces which are used primarily by the authorised user both inside and outside the home and are owned/rented by that user.
11.	Authorisation	An act of empowering an individual or device to perform a specified task.
12.	Authorised Usage	Means the permitted Copying, Moving, and Consumption of Content. (N.B. In all cases the intended usage is private use only and does not include the sale, hire, or Consumption of the Content by an audience who have paid a fee for such Consumption. However, it is not expected that the DVB-CPCM system will be capable of distinguishing private use from other uses).
13.	Back Office	The system of content delivery equipment, network and subscription management systems and usage control systems, including CPCM and/or CA specific equipment as owned, managed and/or supervised by the Service Provider(s).
14.	Backup Copy	A Copy of the original the sole purpose of which is to replace or restore the original if the original becomes lost or damaged. The copy protection status shall not be altered by the Backup Copying process.
15.	Baseline CPCM System	The minimum set of requirements that must be met by a DVB compliant CPCM system.
16.	Capture	Storing the acquired content (to local storage)
17.	Common Interface	Standardised interface between a host device (e.g., a set-top box or DTV) and a removable security module.
18.	Conditional Access	The transport layer system the purpose of which is to ensure that content is accessible in intelligible form only by entities which have obtained the appropriate authorisation
19.	Consumer Electronics	Electronic products bought or rented by the general public.
20.	Consumption	Means viewing of, and/or listening to, Content (and “to Consume” means to view and/or listen to Content).
21.	Content	Video audio, subtitles, images/graphics, animations, webpages, text, games, software (both source code and object code), scripts or any other information which is intended to be delivered to and consumed by a user.
22.	Content Creator	The entity that was the author/composer/performer/or other original creator of the content.

23.	Content Distributor	An entity that acts as the agent for or is the prime distributor of the content The distributor of the content
24.	Content Owner	An entity that owns the intellectual property rights in the content.
25.	Content Protection	The control of access to content and use through usage rights and rules.
26.	Content Protection and Copy Management (CPCM)	The means whereby rights owners can control the copying and/or re-distribution of content which is broadcast or otherwise distributed.
27.	Content Provider	An entity that acts as the agent for or is the prime distributor of the content
28.	Content Reference	A pointer to a specific content item
29.	Content Wrapper	A logical layer accompanying the Content for the purposes of describing and/or protecting it, including without limitation Metadata, CA and Copy Protection. This is distinct from Watermarking.
30.	Copy	Includes any reproduction, duplication, replication, recording, storage, or capture of signals or data for whatever purpose or whatever duration. It is required that CPCM systems will provide means for Authorisation of certain specifically defined types of Copy (e.g. Temporary Copy, Backup Copy etc) , and that such Authorisations will be exercised in conformity with national legislation. N.B. it is important to distinguish between a Copy made within the Authorised Domain and one made outside it in respect of which different entitlements may apply.
31.	Copy Control Not Asserted	Means that the DVB-CPCM system does not assert copy control of the Authorised Usage of that Content : Copying and Consumption of the Content is nonetheless subject to the copyright owned and controlled by the rights owners and their licensees. The technology of the DVB-CPCM system thus needs to take no action in respect to copying of Content thus marked. The right to Move the content for consumption outside the Authorised Domain is addressed in the Usage State below. The “Copy Control Not Asserted” Usage State is intended to cover applications such as Content broadcast by free-to-air/public service broadcasters who wish to allow users to Copy their Content without technical means of enforcement by the DVB-CPCM system.
32.	Copy Never	Means that the Content is not to be Copied (except for incidental and transient copies necessary for the purposes of distribution and/or decoding of the Content: such incidental Copies must be inaccessible to the user and erased as soon as practicable).
33.	Copy No More	has the same effect as “Copy Never” in that the Content thus protected shall not be Copied. However, this Usage State has the purpose of allowing an audit of Copies produced from Copy Once originals.

34.	Copy Once	means that Content received via a broadcast or online distribution ("streaming") may be copied once and once only such that at the end of the copying process there is one Copy only and any other local Copies (e.g. temporary caches/buffer stores) are either erased or made permanently inaccessible. The Copy thus created shall be marked "Copy No More" such that no further Copies can be made from that Copy. This Usage State is intended to cover applications such as online purchase of material to burn onto a local CD-R. It is not applicable where the original Content is supplied on read-only storage media (e.g. DVD).
35.	Copyright	The protection of content by law for defined uses and for defined durations according to international conventions and legislation world-wide.
36.	Data Integrity Verification	Methods and practices to check for unauthorised alteration of data.
37.	Digital Signature	A data element that binds a message or transaction to its originator to verify the integrity of the message or transaction.
38.	Digital Signature Algorithm	An algorithm used in creating the digital signature for a given message (transaction usually involves two parties)
39.	Electronic Program Guide	A means of presenting available content to the consumer, allowing selection of desired content
40.	Encryption	A process of disguising information so that it cannot be recovered by an unauthorised entity.
41.	End-to-end	From the point of content origination to the point of content consumption.
42.	Entitlement Control Message	Message that carries content descrambling keys and a brief description of the content (content ID, date, time, cost, etc.). ECMs are tightly bound with the associated content and may be delivered simultaneously with it.
43.	Entitlement Management Message	Message that specifies service-related authorization levels for the customers. N.B. EMMs are not usually directly related to content items and can be delivered together with or independently from service distribution channels.
44.	Fingerprinting	A process in which every individual content item can be assigned a unique identifier (which can be inserted at many places in the end-to-end system).
45.	Host Security Module	A tamper resistant, hardware security module which connects as a peripheral to a host device. The HSM provides the host with a secure environment in which to perform its cryptographic processing.
46.	In adversarial (passive) Attack	An attack on a system which extracts information and makes use of it, but never injects false information or corrupts any information. See also adversarial attack
47.	Interoperability	The characteristic of entities in a system that allows access and usage seamlessly without loss of functionality or quality
48.	Key	The data which is used by an encryption algorithm to transform plaintext data into encrypted (ciphertext) data, and vice versa. (N.B. does not preclude asymmetric keys)
49.	Key Management	Key generation, distribution, storage, replacement and destruction of keys.

50.	Key Escrow	The retention of encryption keys by a third party so as to allow access to authorised parties (e.g., law enforcement agencies) if third-party decryption of ciphertext is necessary.
51.	Link encryption	Encryption of data transmitted across a link between two devices.
52.	Location Resolution	The process of establishing the address (location and time) of a specific content instance from some unique identifier.
53.	Metadata	"Data about data." Metadata is structured description of content elements, their relationship, form, related usage rules, obligations and options. Metadata may be embedded in or otherwise associated with the content elements.
54.	Move	The process of making a Copy wherein the original is then removed, erased or made no longer accessible. In the case of copy protected content the copy protection status shall not be altered by the Move. N.B. it is important to distinguish between a Move within the Authorised Domain and one outside it in respect of which different entitlements may apply.
55.	Persistent end-to-end control	A CPCM system which allows management of content at any point in the process of capturing/editing/distributing content and which persists through all of these processes including use and distribution within the home network environment
56.	Piracy	Unauthorized use of copyrighted content. Pirates can be grouped in several categories depending on the hacking tools they possess.
57.	Protected Content	Content which is protected by means of a CPCM system.
58.	Public Key Certificate	Data that is digitally signed for the purposes of verifying its integrity. Issuance of certificates may require a Trusted Third Party.
59.	Re-distribution	A process of forwarding content by digital means to another destination outside the domain of the licensed user of the content.
60.	Renewability	The capability to replace, update, re-instate or alter one or more elements of the CPCM system e.g. to allow recovery from a security breach.
61.	Renewable Security	The characteristic of design and implementations that allow for easy, efficient, cost-effective changes to security protocols and security elements.
62.	Return channel	A means of communication between the devices in the consumer domain and the Back Office that also allows interaction and transactions between security elements in the home and the Back Office. For example, modems and a telephone line are commonly used as the return channel in CA systems.
63.	Revocation	The removal of access or usage privileges previously granted by the rights holder.
64.	Securely Bound	Objects that are inextricably linked. For instance content cannot be used without referencing the associated layers of metadata, access control etc.
65.	Serial Copying	Making a Copy of a Copy.
66.	Service Provider	An aggregator and supplier of content which may include gatekeeper & management roles.

67.	Simulcrypt	An architecture that allows a service to be transmitted with the entitlement messages for multiple CA systems. A decoder supporting a particular CA system can extract the relevant entitlement messages and ignore the others.
68.	Spoofing	Pretending to be someone or something else (e.g. using someone else's password).
69.	Super-Distribution	A process in which content is securely Re-Distributed via consumers such that usage by the secondary consumers remains under the control of the rights owners..
70.	Symmetric Encryption	Type of encryption in which encryption and decryption keys are the same or can easily be derived from each other. DES is a well known symmetric encryption algorithm.
71.	Tamper Evident	The property in data security equipment that provides facilities for detecting attempts to tamper with the equipment, and ensures that an appropriate response is made.
72.	Tamper Proof	The property in data security equipment that provides facilities for preventing attempts to tamper with the equipment, and ensures that an appropriate response is made..
73.	Tamper Resistance	The property in data security equipment that provides facilities for resisting attempts to tamper with the equipment, and ensures that an appropriate response is made..
74.	Tamper Resistant System	Systems which are sufficiently difficult/costly to modify to prevent misuse.
75.	Temporary Copy (includes caching)	Certain, specifically defined, "Copies" that are endemic and technologically essential to a system into which content is authorised to be placed - i.e. for a purely transitory instance persisting only so long as necessary to support authorised display and supporting no other purpose of use - will be specifically provided for and authorised for display systems.
76.	Trusted Third Party	A person (or company or other entity) which is trusted by the security organisation and its customers to act as a notary (e.g. to issue and/or to validate certificates)
77.	Usage Rights	The privileges that have been granted by rights holders. Usage rights are associated with specific content elements.
78.	Usage States	Status attached to a piece of content that indicates restrictions placed on the subsequent copying and/or use of that content. "Usage States" are set in CPCM data in accordance with "rules" which are contractually stated by the rights owner to the distributor/broadcaster. Therefore, the application of a rule would typically result in a change of Usage State. The mechanism for this will rely upon subsequent modification to the state set in the DVB-CPCM data. Once set, the Usage State cannot be changed without an operation on it by either the rights owner or their agent.

79.	Usage State Extension	Means additional rules which rights owners may use specify for the Authorised Usage of "Copy Once" Content. Such Usage State Extensions shall be proprietary (i.e. not specified by the DVB) and shall be capable of being decoded only by the appropriate proprietary plug-in connected to the DVB baseline CPCM via the DVB standardised interface. Devices which do not have the appropriate plug-in fitted shall interpret Content with any such Usage State Extensions as "Copy Never" and shall respond accordingly. For the avoidance of doubt, no Usage State other than "Copy Once" shall be subject to modification by a Usage State Extension: in particular this limitation is intended to maintain the unambiguity and integrity of the "Copy Never State".
80.	Usage State Information	means the information, which is distributed (tightly bound to the content) in order to describe the Authorised Usage of that Content.
81.	View	Means to present the content in intelligible form on a display contemporaneously with delivery of the content from a transmission or recorded media and without the production of further copies save for transient incidental copies which cannot be viewed separately.
82.	Watermarking	A method for embedding data electronically within content in such a way as not to compromise the ability to use the content as originally intended but can later be detected electronically e.g. to establish the provenance of content.